REMARKS

Claims 1-87 are pending in this application. Of these, claims 1, 20, 33, 40, 59, and 71 are independent. Favorable reconsideration and further examination are respectfully requested.

Claim Objections

The Examiner objected to claim 32 as reciting improper antecedent basis for the term "the unlocked data." Applicants have amended claim 32, which depends on claim 20, to replace the term "the unlocked data" with the term "the master data set," which is recited in claim 20. Accordingly, claim 32 as amended recites proper antecedent basis.

Claim Rejections under 35 U.S.C. § 101

The Examiner rejected claims 1, 5-8, 10-33, 36-70, and 79-87 under 35 U.S.C. 101 as being directed to non-statutory subject matter.

Applicants have amended independent claims 1, 20, and 33 to recite a "computer-implemented" method and to include features of associated computer hardware that execute the methods (e.g., memory, and a computer system). Applicants have amended independent claims 40, 59, and 71 to recite that the computer program product is tangibly stored one or more computer-readable medium storage devices (e.g., non-volatile memory such as EPROM). Accordingly, Applicants respectfully request withdrawal of the 101 rejections.

Claim Rejections under 35 U.S.C. § 102 and 103

Turning to the art rejections, claims 20-30 and 59-69 were rejected under 35 U.S.C. 102(b) over Carter et al. (U.S. Pat. 5,418,945). Claims 1-5, 7-19, 31-34, 36-44, 46-58, 70-72, and 74-77 were rejected under 35 U.S.C. 103 over Carter and Fabbio (U.S. Pat. 5,335,346). Claims 90-81, 85, and 86 were rejected under 35 U.S.C. 103 over Carter and Sweeney et al. (U.S. Pat. 5,966,715). Claims 6, 35, 45, 73, 78, 79, 82-84, and 87 were rejected under 35 U.S.C. 103 over Carter, Fabbio, and Sweeney.

As shown above, Applicant has amended the claims to define the invention with greater clarity. In view of these clarifications and the arguments below, reconsideration and withdrawal of the art rejections are respectfully requested.

Independent claims 1 and 40

Claim 1 as amended requires the first entity to have permission to change the unlocked data set and to view but *not* to change the locked data set, before access to the stored data set is provided to the second entity. However, while access is provided to the second entity (in which the second entity can modify the unlocked data set), claim 1 requires that the first entity be *denied* permission to change the unlocked data set and *granted* permission to modify the locked data set.

In this regard, as described in Applicants' specification in FIG. 3 and accompanying text on page 9, line 24 to page 10, line 5, the locked and unlocked data of the stored data set maintained by the first entity become reversed in the second entity after access to the data is provided to the second entity. Denying permission to the first entity to change the unlocked data,

when it is made available to be changed by the second entity, ensures that both the first and second entities do not attempt to change the unlocked data at the same time. For example, as described in Applicants' specification at page 5, lines 4-5, the method of claim 1 helps to avoid situations where there are overlapping edits that need to be reconciled. Granting the first entity permission to changed the clocked data allows different portions of a data set to be modified at the same time by different entities (e.g., simultaneously, the second entity can change unlocked data but not the locked data and the first entity can change the locked data but not the unlocked data). The applied art is not believed to disclose or to suggest the features of claim 1.

In this regard, Carter describes a system in which a state means allows only one client to modify a data set (e.g., a master file group) at a time by locking the *entire* master file group to other clients during the time the client is modifying the data. Nowhere does Carter disclose or suggest allowing different portions of a master file group to be modified at the same time. Rather, in Carter, only one client is provided permission to change a master file group at any given time. For example, the passages of Carter at col. 5, lines 22-26, and at lines 65-66, describe the locking and unlocking of a master file group:

> State means 43 ensures that only one client has a copy of third master file group 19 checked out for alteration, were third master file group 19 already in a locked state then the check out request would be denied ... State means 43 then unlocks third master file group permitting check outs for further changes."

There is nothing in the above passage or anywhere else in Carter that describes, for example, enabling a first client to modify a locked portion of a master file group while a second client modifies an unlocked portion of the same master file group.

Fabbio and Sweeney do not remedy the foregoing deficiencies of Carter with respect to claim 1. In this regard, Fabbio describes a system for granting a user write or read access to individual data objects by comparing the credentials of the user with access controls assigned to the objects. However, Fabbio does not disclose or suggest, for example, granting two different users write access to different portions of a data object at the same time.

Sweeney describes an acyclic graph architecture that provides users access to date based on permissions associated with the users' respective database groups, e.g., see col. 5, line 13 to col. 6, line 5. Sweeney, however, does not disclose or suggest granting permission to modify locked data of a data set to a first user while also granting permission to a second user to modify unlocked data of the data set.

Claim 40 recites limitations that are similar to the limitations of claim 1. Accordingly, for at least the foregoing reasons, claims 1 and 40 are believed to distinguish over the applied art.

Independent claims 20 and 59

Claim 20 as amended requires permissions that indicate the operations that a second entity may perform on a first subset of data within a master data set, and that the permissions be included in the first subset of data and indicate applications that the second entity may use for manipulating the first subset of data. Applicants' specification on page 7, lines 20-21, and on page 8, lines 1-4, describe permissions included in the locked and unlocked data sets of a master data set. For example, the locked data set can include information that the second entity has access to but does not have permission to change. Furthermore, the unlocked data set can

include a variety of permissions for manipulation, such as permissions to read data, add new data with in the unlocked data set, and change or delete existing data in the unlocked data set. Applicants' specification at page 8, lines 15-17 describe a locked data set including identifiers of applications that an entity may use to manipulate data within the master data est. The applied art is not believed to disclose or to suggest the features of claim 1.

In this regard, Carter describes a system in which a security means 39 (shown in FIG. 2) controls access of a client or server (e.g., client 11, server 12 or server 14) to data stored in a data base 17. FIG. 2 of Carter has been reproduced below for reference.

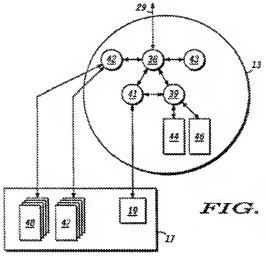

FIG. 2

According to the passage of Carter at col. 4, lines 50-58, the security means, rather than the data in the database 17, includes access permissions, in the form of access and write password lists:

> Server means 38 provides the sole access to second resident database 17, and is designed to respond only to requests from client 11, server 12, or server 14. Once a transaction request is received from client 11, server 12, or server 14, the request is first validated by security means 39. Security means 39 maintains an access password 44 and a write password list 46. Security means 39 allows access through server means 38 only if the transaction request provides access password 44.

Nowhere does the foregoing passage or anywhere else in Carter disclose or suggest including permissions for manipulating a subset of data of a master data set in the subset of data itself. Rather, in Carter, clearly the permissions are maintained in a security means 39 that lies outside of the database 17. Furthermore, there is nothing in Carter that describes or suggests, for example, including the password lists in a subset of data accessed from the database 17. Carter also does not disclose or suggest that the permissions (e.g., password lists) indicate applications that an entity may use for manipulating a subset of data in the database 17.

Fabbio and Sweeney do not remedy the foregoing deficiencies of Carter with respect to claim 20. In this regard, Fabbio describes a system in which a data object manager controls users' access to and modification of data objects using access control lists that describes various permissions (e.g., read, write, execute) assigned to the users for the data objects. FIG. 4 of Fabbio and the accompanying text at col. 7, lines 49-57 describe the access control list in further detail:

> The access control attributes on each object consists of eight 32 bit entries 111-118, of which seven of these entries 111-117 represent the user or group ids making up the access control list 100. The eighth entry 118 is divided into eight 4-bit slots 121-128, where the first seven slots 121-127 represent the privileges associated with the corresponding access control entry 111-117. The eighth 4-bit slot 128 is used to keep the count of the number of entries used. In the first seven 4-bit slots 121-127, the first three bits represent read, write, and execute privileges while the last bit of the 4-bit slot indicates whether the corresponding access control entry applies to a user or a group id.

The access control list of Fabbio is nowhere disclosed or suggested to indicate applications that a user may use for manipulating the data object. For example, the access control list does not include an id of an application, but rather, includes an id only for an individual user or a group of users.

Sweeney describes a database security system that determines which version of an application should be provided to a user and ensures that the user receives the correct version of the application. In Sweeney, however, the applications to be used are identified by an external server rather than by permissions included in a subset of data being accessed in the database. For example, the passage of Sweeney at col. 9, lines 6-11 describes a "Launch" application that sends a request to an external server regarding the applications that a user should use:

> With the correct name and password, Launch connects to the server and asks the server what set of applications the user is allowed to use. Launch receives a list of applications that the user is allowed to access. The user picks an application and Launch asks the server what version of the application is the correct version for that user. These two steps may be combined into one query or may be two separate queries.

Nowhere does Sweeney, for example, disclose or suggest that the data retrieved from the database indicates the applications a user should use for manipulating the data. Claim 59 recites limitations that are similar to the limitations of claim 20. Accordingly, for at least the foregoing reasons, claims 20 and 59 are believed to distinguish over the applied art.

Independent claims 33 and 71

Claim 33 as amended requires permissions that indicate the operations that a second entity may perform on unlocked data within a master data set, that the permissions be included in

the unlocked data, and that the permissions indicate applications that the second entity may use for manipulating the unlocked data. As described above, neither Carter, Fabbio, nor Sweeney disclose or suggest permissions included in a subset of data (e.g., unlocked data) within the master data set where the permissions indicate the operations that a second entity may perform on the subset of data within a master data set and applications that the second entity may use for manipulating the subset of data. Claim 71 recites limitations that are similar to the limitations of claim 33. Accordingly, for at least the foregoing reasons, claims 33 and 71 are believed to distinguish over the applied art.

Each of the dependent claims is also believed to define patentable features of the invention. Each dependent claim partakes of the novelty of its corresponding independent claim and, as such, has not been discussed specifically herein.

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claims, except as specifically stated in this paper, and the amendment of any claims does not necessarily signify concession of unpatentability of the claim prior to its amendment.

In view of the foregoing amendments and remarks, Applicants respectfully submit that the application is in condition for allowance, and such action is respectfully requested at the Examiner's earliest convenience.

Applicants' undersigned attorney can be reached at the address shown below. All telephone calls should be directed to the undersigned at 617-521-7896.

Enclosed is a one-month Petition for Extension of Time fee. Please apply any other charges or credits to deposit account 06-1050, referencing Attorney Docket No. 13907-021002.

Respectfully submitted,

Date: June 27, 2007

Paul A. Pysher
Reg. No. 40,780

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906